대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 64187 호
Application Number PATENT-2001-0064187

출 원 년 월 일 : 2001년 10월 18일
Date of Application OCT 18, 2001

출 원 인 : 한국전자통신연구원
Applicant(s) KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INS

2002 년 01 월 10 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0004
【제출일자】	2001.10.18
【발명의 명칭】	공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법
【발명의 영문명칭】	METHOD FOR ISSUING A CERTIFICATE OF AUTHENTICATION USING INFORMATION OF A BIO METRICS IN A PKI INFRASTRUCTURE
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2001-038646-2
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2001-038648-7
【발명자】	
【성명의 국문표기】	김희선
【성명의 영문표기】	KIM,Hee Sun
【주민등록번호】	751015-2262118
【우편번호】	305-350
【주소】	대전광역시 유성구 가정동 236-1 구 332
【국적】	KR
【발명자】	
【성명의 국문표기】	김태성
【성명의 영문표기】	KIM,Taesung
【주민등록번호】	721202-1221829
【우편번호】	305-803

【주소】 대전광역시 유성구 송강동 200-1 한솔아파트 203-705
【국적】 KR
【발명자】
【성명의 국문표기】 노종혁
【성명의 영문표기】 ROH,Jong-Hyuk
【주민등록번호】 700420-1143627
【우편번호】 405-840
【주소】 인천광역시 남동구 구월3동 1376-7
【국적】 KR
【발명자】
【성명의 국문표기】 최대선
【성명의 영문표기】 CHOI,Dae Seon
【주민등록번호】 730302-1069411
【우편번호】 302-280
【주소】 대전광역시 서구 월평동 황실타운 118-905
【국적】 KR
【발명자】
【성명의 국문표기】 조영섭
【성명의 영문표기】 CHO,Young Seob
【주민등록번호】 691212-1155513
【우편번호】 305-804
【주소】 대전광역시 유성구 신성동 142-11 상가주택 301호
【국적】 KR
【발명자】
【성명의 국문표기】 조상래
【성명의 영문표기】 CHO,Sang Rae
【주민등록번호】 711023-1037015
【우편번호】 305-752
【주소】 대전광역시 유성구 송강동 송강청솔아파트 512-1408
【국적】 KR

【발명자】

【성명의 국문표기】	진승헌
【성명의 영문표기】	JIN,Seung Hun
【주민등록번호】	680723-1037010
【우편번호】	302-752
【주소】	대전광역시 서구 월평2동 백합아파트 104동 1405호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 장성구 (인) 대리인 김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	8	항	365,000 원
【합계】	394,000 원		
【감면사유】	정부출연연구기관		
【감면후 수수료】	197,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법에 관한 것이다. 즉, 본 발명은 공개키 기반 인증시스템에서 인증서 발급에 있어서, 인증서 발급 요청시에 요청 메시지의 보호를 위해 발급시 요구되는 인가코드를 등록단계가 아닌 인증서 발급 요청 단계에서 사용자의 생체정보를 통한 사용자 인증시 인증기관으로부터 부여되도록 함으로써 사용자 입장에서 인증서 발급시 복잡한 인가코드를 기억하고 입력하지 않아도 되도록 함으로써 인증서 발급 절차를 간소화할 수 있으며, 또한 인증서 발급단계에서 생체정보를 이용하여 인가코드를 부여함에 따라 제3자에 의해 인증서 발급단계 이전에 참조번호가 노출되었다 하더라도 인가코드를 받기 위해서는 생체정보에 의한 실시간 신원확인 절차가 필요하게 되어 제3자에 의한 인증서 발급시도가 방지됨으로써 인증서 발급시 더 높은 보안성을 유지할 수 있게 되는 이점이 있다.

【대표도】

도 4

【색인어】

공개키, 인증시스템, 생체정보, 인증서 발급

【명세서】

【발명의 명칭】

공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법
{METHOD FOR ISSUING A CERTIFICATE OF AUTHENTICATION USING INFORMATION OF A BIO METRICS IN A PKI INFRASTRUCTURE}

【도면의 간단한 설명】

도 1은 본 발명의 실시 예에 따른 공개키 기반 구조 인증시스템의 네트웍 구성을 도시한 것이다.

도 2는 본 발명의 실시 예에 따른 사용자 시스템의 개략적인 블록 구성을 도시한 것이다.

도 3은 본 발명의 실시 예에 따른 인증기관 서버의 개략적인 블록 구성을 도시한 것이다.

도 4는 본 발명의 실시 예에 따른 사용자 시스템과 인증기관 서버간 인증서 발급을 위한 동작 제어 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<5> 본 발명은 공개키 기반 구조(PKI: Public Key Infrastructure) 인증시스템에 관한 것으로, 특히 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법에 관한 것이다.

<6> 통상적으로, 공개키 기반 구조는, 인터넷상 보안이 요구되는 전자문서의 송/수신시 상기 인증시스템에 의해 인증된 회원 사용자간에 공개키와 개인키를 이용한 암호화 전송이 가능하도록 하는 시스템을 말하는 것으로, 즉, 상기 인증시스템에 회원 등록된 사용자들은 해당 인증기관으로부터 정당한 사용자임을 인증하는 디지털 인증서를 발급받고 상대방 공개키로 보안이 요구되는 전자문서를 암호화한 후, 자신의 개인키로 전자서명하여 전송함으로써 상기 인증시스템에 회원 등록된 사용자간에는 전자문서를 안전하게 송/수신할 수 있도록 하는 시스템을 말한다.

<7> 이때 종래 인증시스템에서 인증서 발급 단계에서는 인증서를 발급 받기 위해서는 먼저 사용자의 신원 및 인증서 발급 권한을 판단하여야 하며, 또한 사용자가 자신의 개인키와 공개키에 대한 공개키쌍을 생성하여 생성한 공개키의 인증서를 발급 받기 위해서는 해당 공개키에 대응되는 개인키를 소유하고 있음을 증명하는 키소유증명(POP:Proof Of Possession of private key)을 수행하여야 하는데, 이를 위해서는 사용자가 상기 인증시스템에 사용자 등록 단계에서 상기 인증기관과 연결되는 등록기관에 가서 사용자 등록을 요청한 후, 인증시스템에 연결할 수 있는 참조번호와 인가 코드를 수신하고 자신의 사용자 시스템을 통해 상기 참조번호와 인가코드를 입력하여야만 인증서 발급이 가능하였다.

<8> 그러나 상기 인증서 발급을 위해 필요되는 인가 코드는 타인에 의해 추측이 불가능하도록 큰 비트수의 복잡한 값으로 결정되기 때문에 사용자가 이를 등록기관으로부터 통보 받아 완전히 숙지해서 사용하기에는 큰 어려움이 있었으며, 이를 위해 종래 등록기관이 상기 인가코드를 사용자 이메일로 전송하여 준다거나

또는 용지에 인쇄하여 주는 방법이 관행적으로 수행되어 왔으나, 이는 참조번호와 인가코드가 중간에 노출될 위험이 크며, 악의를 가진 타인에 의해 노출되는 경우 제3자에 의한 악의적인 도용의 위험성이 있었다. 또한 인증서 발급 요청시 인가코드 입력에 따른 인증서 발급 절차가 복잡하였던 문제점이 있었다.

<9> 한편, 상기와 같은 공개키 기반 구조 인증시스템에서의 인증서 발급방법으로는 출원번호 1999-0051586호에 개시된 '인증기관 시스템의 사용자용 공개키 인증서 생성방법'과 2000년 10월에 출판된 '한국통신학회지' 제17권 10호 105~117페이지에 개시된 '전자서명 인증기술동향' 등과 같은 공개키 기반 구조에서의 인증기술이 개시되어 있으나, 상기 '인증기관 시스템의 사용자용 공개키 인증서 생성방법'에는 단지 인증기관에서 사용자에게 신속하게 공개키 인증서를 생성하는 방법이 개시되어 있으며, '전자서명 인증 기술동향'에는 단지 공개키 기반 구조 구현에 필요한 표준 및 CMP를 이용한 종래 통상적인 인증서 발급 방법이 개시되고 있을 뿐 상기한 종래 공개키 기반 구조 인증시스템에서와 마찬가지로 인증서 발급 요청시 복잡한 인가코드의 사용으로 인한 인증서 발급 절차의 불편함과 인증서 발급 단계에서 인가코드의 노출 위험은 여전히 문제점으로 남아 있었다.

【발명이 이루고자 하는 기술적 과제】

<10> 따라서, 본 발명의 목적은 공개키 기반 구조 인증시스템에서 생체정보를 이용한 사용자 인증을 통해 인증서 발급이 가능하도록 함으로써, 사용자가 복잡한 인가코드를 직접 입력하지 않고도 쉽게 인증서 발급을 요청할 수 있도록 하며, 또한 생체정보를 이용한 사용자 인증을 통해 인증서 발급 절차의 보안성도 높일 수 있도록 하는 인증서 발급 방법을 제공함에 있다.

<11> 상술한 목적을 달성하기 위한 본 발명은 등록기관, 인증기관, 사용자 시스템을 포함하는 공개키 기반 구조 인증시스템에서 사용자 시스템과 인증기관간 생체정보를 이용하여 인증서를 발급하는 방법에 있어서, (a)인터넷을 통해 상기 인증시스템에 접속한 상기 사용자 시스템으로부터 인증서 발급 요청 메시지를 수신하는 단계; (b)상기 인증서 발급 요청을 위한 사용자 인증을 위해 상기 사용자 시스템으로부터 전송되는 해당 사용자의 참조번호와 생체정보를 추출하는 단계; (c)상기 전송된 사용자의 생체정보와 데이터 베이스 저장부내 등록 저장된 상기 참조번호에 해당하는 회원 등록 사용자의 생체정보가 일치하는지 여부를 검사하는 단계; (d)상기 생체정보가 일치하는 경우 회원 등록시 상기 참조번호와 함께 생성된 상기 인증서 요청 사용자의 인가코드를 독출하여 사용자 시스템으로 제공하는 단계; 및 (e)사용자 시스템으로부터 생성된 공개키를 수신하여 인증서를 발급하는 단계;를 포함하여 진행하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<12> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예의 동작을 상세하게 설명한다.

<13> 도 1은 본 발명의 실시 예에 따른 공개키 기반 구조 인증시스템의 네트웍 구성을 도시한 것이다. 이하 상기 도 1을 참조하면, 공개키 기반 구조 인증시스템은, 사용자의 신원을 대행 확인하는 등록기관, 상기 등록기관에 의해 등록 요청된 사용자에 대한 참조번호와 인가코드를 생성하고, 인증서를 발급하는 인증기관 및 인터넷을 통해 상기 인증기관과 접속되어 온라인으로 사용자 공개키에 대한 인증서 발급을 요청하는 사용자 시스템으로 구성된다.

<14> 먼저 등록기관(100)은 인증기관(102)과 물리적으로 멀리 떨어져 있는 사용자들을 위해 인증기관(102)과 인증서 요청 객체 사이에 존재하여 사용자들의 인증서 요청시 인증기관(102) 대신 그들의 신분과 소속을 확인하는 기능을 수행하는 시스템으로, 인터넷(106)을 통해 인증기관(102)과 연결되어 사용자의 상기 인증시스템 회원 등록 요청을 인증기관(102)으로 요청하고 등록 승인 여부를 수신하여 해당 사용자에게 인증서 발급 요청시 사용자 인증을 위한 참조번호를 통보하여 준다.

<15> 사용자 시스템(104)은 PC(Personal Computer) 등과 같이 인터넷(106)에 접속할 수 있는 단말장치를 말하는 것으로, 사용자(110)는 상기 등록기관(100)을 통한 상기 인증시스템의 인증서 발급 요청시 해당 등록기관(100)으로부터 통보된 참조번호와 자신의 생체정보를 이용하여 인증기관(102)에 접속한 후, 사용자 시스템(104)에서 생성되는 사용자의 공개키에 대한 인증서 발급을 요청하게 된다.

<16> 특히 본 발명의 실시 예에서는 사용자 시스템을 이용한 인증서 발급 요청시 상기 참조번호와 생체정보만을 이용하여 회원 인증이 수행이 가능하도록 함으로써 인증서 발급을 위해 인증기관 접속시 필요하게되는 복잡한 인가코드를 사용자가 일일이 숙지하지 않아도 됨으로써 사용자 입장에서는 인증서 발급 요청을 위한 회원 인증 과정이 간소화되며, 인증기관 입장에서는 생체정보를 이용한 회원 인증을 통해 보다 신뢰성 높은 보안서비스를 유지하게 되는 것이다.

<17> 도 2는 상기 도 1에 도시된 사용자 시스템(104)의 개략적인 블록 구성을 도시한 것이다. 상기 도 2를 참조하면, 제어부(204)는 상기 사용자 시스템(104)의 전반적인 동작을 제어하며, 본 발명의 실시 예에 따라 상기 인증기관 접속시 인

증기관(102)으로부터 제공되는 인증시스템 회원 사용자를 위한 웹페이지 화면을 다운로드받아 모니터부(200)에 디스플레이시키며, 사용자로부터의 인증서 발급 요청이 있는 경우 사용자의 생체정보를 입력받아 인증기관(102)으로 상기 인증서 발급 요청 메시지와 생체정보 입력장치로 구비되는 지문입력장치(108)를 통해 입력되는 사용자 고유의 지문정보를 전송시켜서 인증서 발급을 요청한다.

<18> 메모리부(206)는 제어부(204)의 동작에 필요한 각종 운영 프로그램을 내장하며, 상기 운영 프로그램의 구동시 필요한 각종 기본 데이터를 저장하고 있는 롬(ROM:Read Only Memory)과 제어부(204)의 제어에 의해 동작되는 프로그램을 임시 저장하거나 상기 동작 프로그램 수행시 발생되는 데이터를 일시 저장하기 위한 램(RAM:Random Access Memory)으로 구성된다. 통신부(208)는 상기 제어부(204)의 제어에 따라 상기 인증서 발급 요청 메시지를 해당 인증기관(102)으로 전송시키며, 상기 인증기관(102)과 사용자 시스템(104)간 인터넷(106)을 통해 송/수신되는 데이터를 인터페이스한다. 키입력부(202)는 사용자 인터페이스부로 다양한 숫자키 및 기능키를 구비하며 사용자로부터의 키입력 발생시 해당 키이벤트 데이터를 발생시켜 제어부(204)로 인가시킨다. 모니터부(200)는 제어부(204)의 제어에 따른 사용자 시스템(104)의 각종 동작 상태를 디스플레이시킨다. 지문정보 입력장치(108)는, 지문센서를 통해 사용자의 지문을 스캔 입력하는 지문인식부(212)와 상기 지문인식부(212)로부터 스캔 입력된 사용자 고유의 지문데이터를 분석하여 사용자

고유의 지문특징값을 추출하여 제어부(204)로 인가시키는 지문처리부(210)로 구성된다. 한편, 본 발명의 실시 예에서는 상기 생체정보 입력장치로 사용자의 지문을 인식하는 지문정보 입력장치를 예시하였으나, 이는 설명의 편의상 일 예를 들어 설명한 것 일뿐 상기 생체정보는 사용자의 홍체 정보나 얼굴특징 벡터값 등 다양한 사용자 고유의 생체정보가 될 수 있다.

<19> 인증기관(102)은 상기 공개키 기반 인증시스템의 핵심 객체로서 인증서 등록 발급 조회시 인증서의 정당성에 대한 관리를 총괄하는 시스템으로, 인터넷 뱅킹 등과 같이 보안이 요구되는 인터넷을 통한 전자문서의 송/수신시 상기 인증시스템에 회원 등록된 사용자를 인증하는 디지털 인증서를 발행하여 공신력 있는 제3자의 인증서를 통한 보다 안정성 있는 전자문서 전송 서비스를 제공하며, 특히 본 발명의 실시 예에서는 상기 인증서 발급에 있어서 사용자 시스템으로부터의 인증서 발급 요청이 있는 경우 생체정보를 이용하여 회원 사용자를 인증하고 상기 사용자에 대한 인가코드를 생성하여 사용자 시스템으로 제공함으로서 사용자가 인증서 발급 요청시 인가코드를 입력하지 않아도 되도록 하여 인증서 발급 절차를 간소화시킨다.

<20> 도 3은 상기 도 1의 인증기관 서버(102)의 개략적인 블록 구성을 도시한 것이다. 이하 상기 도 3을 참조하여 인증기관 서버(102)의 동작을 보다 상세히 설명하기로 한다. 먼저 분석 모듈부(300)는 서버 제어부(302)의 제어에 따라 상기 사용자 시스템(104)으로부터 암호화되어 전송된 인가코드 요청 메시지 또는 인증서 발급 요청 메시지를 복호화시키고 사용자의 생체정보에 대한 기밀성을 검사한다. 메시지 생성 모듈부(304)는 서버 제어부(302)의 제어에 따라 상기 인증서 발

급 요청 메시지에 대한 인증서 발급이 정상적으로 수행되었음을 알리는 응답메시지 또는 생체정보의 불일치로 인한 인증서 발급에 에러가 발생했음을 알리는 오류메시지를 생성한다. 서명모듈부(308)는 상기 발급된 인증서를 인증기관(102)의 개인키로 전자서명을 수행한다. 암호모듈부(306)는 상기 인증기관으로부터 등록기관 또는 회원 사용자 시스템으로 전송되는 메시지에 대해 해당 등록기관 또는 사용자 시스템의 공개키로 암호화를 수행한다.

<21> 서버 제어부(302)는 상기 인증기관 서버(102)의 전반적인 동작을 제어하며, 특히 본 발명의 실시 예에 따라 상기 인증시스템의 회원 사용자로부터 인증서 발급 요청 수신시 해당 사용자 시스템(104)으로부터 전송된 회원 사용자의 생체정보를 검사하여 회원 사용자에 대한 인증을 수행하며, 상기 생체정보를 통해 상기 인증서 발급을 요청한 회원 사용자가 정당한 사용자로 판정되는 경우 상기 사용자에 대한 인가코드를 이용하여 인증서를 발급하고 상기 메시지 생성 모듈부(304)를 제어하여 인증서 발급 요청이 정상적으로 처리되었음을 알리는 응답메시지를 생성시키며, 암호모듈부(306)와 서명모듈부(308)를 제어하여 상기 인증서 내용이 전송 중 외부로 노출되지 않도록 보호하고 인증기관(102)의 개인키로 전자서명을 수행하여 해당 사용자 시스템(104)으로 온라인 전송시킨다.

<22> 데이터 베이스 저장부(114)는 상기 인증기관 서버(102)에 의해 참조되며, 상기 인증시스템에 회원 가입된 사용자 정보와 인증서 발급을 위한 참조번호를 구비한 사용자 정보 DB(310)와, 상기 해당 사용자에 대한 생체정보를 상기 사용자 정보와 연계되도록 저장하고 있는 생체정보 DB(312)와, 상기 회원 사용자들에게 발급된

인증서 정보를 구비한 인증서 DB(314) 등 상기 인증기관 서버(102) 운영에 따른 각종 DB를 구비한다. 메모리(314)는 서버 제어부(302)의 동작에 필요한 각종 운영 프로그램을 내장하며, 상기 운영 프로그램의 구동시 필요한 각종 기본 데이터를 저장하고 있는 롬(ROM:Read Only Memory)과 서버 제어부(302)의 제어에 의해 동작되는 프로그램을 임시 저장하거나 상기 동작 프로그램 수행시 발생되는 데이터를 일시 저장하기 위한 램(RAM:Random Access Memory)으로 구성된다. 통신부(316)는 상기 서버 제어부(302)의 제어에 따라 상기 사용자 시스템(104)으로부터의 인증서 발급 요청에 따른 응답메시지와 해당 인증서를 해당 사용자 시스템(104)으로 전송시키며, 상기 사용자 시스템(104)과 인증기관 서버(102)간 인터넷(106)을 통해 송/수신되는 데이터를 인터페이스한다.

<23> 도 4는 본 발명의 실시 예에 따라 참조번호와 생체정보를 이용하여 인증서를 발급 받기 위한 사용자 시스템과 인증기관에서의 동작 제어 흐름을 도시한 것이다. 이하 상기 도 1, 도 2, 도 3 및 도 4를 참조하여 상세히 설명한다.

<24> 먼저 사용자는 상기 인증시스템에 회원으로 등록하고자 하는 경우 등록기관(100)으로 가서 회원 등록을 요청하고 회원 등록을 위한 사용자 신원 확인시 필요한 각종 사용자 신상정보 및 본 발명의 실시 예에 따른 생체정보를 이용한 인증서 발급을 위해 생체정보를 입력하여 회원 등록을 요청하게 된다. 이에 따라 상기 등록기관(100)은 상기 회원 등록 요청한 사용자의 신원을 인증기관(102)을 대신하여 신원확인 대행하며, 신원 확인된 사용자에 대해 상기 사용자 정보와 생체정보를 전송하여 회원 등록을 요청하게 되고, 상기 사용자의 회원 등록 승인에 따라

생성되는 참조번호를 인증기관(102)으로부터 수신하여 사용자에게 제공한다. 상기 참조번호라 함은 인증기관(102) 회원 등록 승인에 따라 회원 등록 요청한 사용자에게 부여하는 번호로서 사용자가 인증기관(102)으로부터 인증서 발급을 요청하기 위해 자신의 사용자 시스템(104)을 이용하여 인증기관(102)에 접속할 시 회원 인증을 받기 위해 필요한 참조정보가 된다. 여기서 종래에는 상기 참조번호와 함께 인가코드도 사용자에게 발급하여 사용자가 인가코드를 직접 입력하도록 하여 회원 인증을 수행하도록 하였으나, 상기 인가코드는 보안을 위해 상당히 복잡한 코드로 구성되어 사용자가 이를 숙지하거나 인증기관 접속시 입력하는데 번거로우며, 또한 인가코드 도용의 위험성이 있었음을 전술한 바와 같다. 따라서 본 발명의 실시 예에서는 등록기관(100)에서는 사용자에게 참조번호만을 발급하도록 하며, 사용자가 인증시스템 접속시 생체정보를 이용한 사용자 인증시 인증기관(102)이 인가코드를 생성하여 제공하도록 한다.

<25> 상기와 같이 인증시스템에 회원 등록을 요청한 사용자는 이제 사용자 시스템(104)을 이용하여 인증시스템에 접속한 후, 인터넷 뱅킹, 웹보안메일 등과 같은 보안서비스 이용을 위한 개인키/공개키의 생성을 위해 인증기관(102)으로부터 인증서를 발급 받는 과정을 먼저 수행하여야 한다.

<26> 이제 사용자가 사용자 시스템을 이용해 온라인으로 인증서를 발급 받는 구체적인 동작을 살펴보기로 한다. 즉, 사용자는 사용자 시스템(104)을 이용하여 인터넷(106)을 통해 인증기관(102)에 접속하고 상기 등록기관(102)으로부터 발급받은 참조번호와 자신의 생체정보 입력을 통해 회원 인증을 수행시키게 된다. 이에 따라

사용자 시스템(104)은 (S400)단계에서 상기 인증기관 접속 요구에 따라 인터넷(106)을 통해 해당 인증기관 서버(102)로 접속하여 인증시스템의 웹페이지화면을 모니터부(200)를 통해 디스플레이시키게 된다.

<27> 이에 따라 상기 웹페이지화면에서 사용자는 상기한 바와 같이 회원 인증을 위해 상기 등록기관으로부터 발급받은 참조번호 및 생체정보를 입력하게 되는데, 그러면 사용자 시스템(104)은 (S402)단계에서 상기 키입력부(202)를 통해 입력되는 사용자의 참조번호를 입력받고, (S404)단계에서 지문입력장치(108)로부터 입력되는 사용자의 고유의 생체정보 중 하나인 지문정보를 입력받는다. 이어 사용자 시스템(104)은 (S406)단계로 진행해서 인가코드 요청 메시지를 생성하여 (S408)단계에서 상기 인증기관(102)의 공개키로 이를 암호화한 후, (S410)단계로 진행해서 상기 참조번호와 생체정보를 포함한 인가코드 요청 메시지를 인증기관 서버(104)로 전송하고, (S412)단계에서 인증서 발급 요청을 위한 인가코드 수신을 대기한다.

<28> 그러면 인증기관 서버(102)는 (S500)단계에서 상기 사용자 시스템(104)으로부터 전송된 인가코드 요청 메시지를 수신하고 (S502)단계에서 상기 분석 모듈부(300)를 제어하여 상기 사용자 시스템(104)으로부터 암호화되어 전송된 인가코드 요청 메시지를 복호화하여 인가코드 요청 정보의 기밀성을 검사하며, 이어 (S504)단계로 진행해서 상기 인가코드 요청 메시지에 포함된 참조번호 및 생체정보를 분석하여 데이터 베이스 저장부(114)내 생체정보 DB(312)에 저장된 상기 전송된 참조번호에 해당하는 사용자의 생체정보가 상기 전송된 생체정보와 동

일한지 여부를 검사하여 상기 접속한 사용자가 정당한 사용자인지 여부를 검사한다.

<29> 이때 만일 상기 접속한 사용자의 생체정보가 회원 등록된 상기 참조번호의 사용자 생체정보와 일치하지 않는 경우 인증기관 서버(102)는 (S506)단계에서 이에 응답하여 (S508)단계로 진행해서 상기 메시지 생성모듈부(304)를 제어하여 상기 인가코드 요청을 정상적으로 수행할 수 없음을 알리는 인가코드 요청 오류 메시지를 생성하여 사용자 시스템(104)으로 전송시킨다. 이와 달리 상기 접속한 사용자의 생체정보가 회원 등록된 상기 참조번호의 사용자 생체정보와 일치하는 경우 인증기관 서버(104)는 (S510)단계로 진행해서 회원 등록 승인시 상기 참조번호와 함께 생성되어 저장된 인가코드를 독출하여, (S512)단계에서 상기 인가코드를 사용자 시스템(104)으로 송신시키고, (S514)단계에서 인증서 발급을 위한 사용자로부터의 공개키 수신을 대기한다.

<30> 그러면 사용자 시스템(104)은 (S414)단계에서 상기 인가코드를 수신하고 (S416)단계에서 인증시스템을 통한 보안서비스에 사용할 사용자의 개인키와 공개키를 생성시킨다. 이어 사용자 시스템(104)은 (S418)단계에서 인증서 발급을 요청하는 메시지를 생성하고, 상기 인가코드로 상기 인증서 발급 요청 메시지를 보호하여 상기 공개키 정보와 함께 상기 인증기관 서버(102)로 전송하게 된다.

<31> 이에 따라 인증기관 서버(102)는 (S516)단계에서 상기 사용자 시스템(104)으로부터의 인증서 발급 요청을 수신하고, (S518)단계에서 상기 분석 모듈부(300)를 제어하여 상기 인증서 발급 요청 메시지를 복호화한 후, 인증서 발급 요청 정보의 기밀성을 검사하며, (S520)단계에서 상기 사용자 시스템(104)으로부터

수신된 공개키에 대해 키소유증명 과정을 수행하여 사용자가 상기 공개키에 대응되는 개인키를 소유하고 있는지 여부를 검사한다. 이어 인증기관 서버(102)는 (S522)단계에서 인증서를 생성하여 인증서 DB(314)에 저장시키고, (S524)단계에서 암호모듈부(306)와 서명모듈부(308)를 제어하여 상기 사용자에게 발급된 인증서와 상기 인증서 발급이 정상적으로 처리되었음을 알리는 응답메시지를 상기 인가코드로 보호하고, 인증기관(102)의 개인키로 전자서명하여 사용자 시스템(104)으로 전송시킨다. 이에 따라 사용자 시스템(104)은 (S420)단계에서 상기 인증서를 수신하여 사용자에게 디스플레이 시켜 인증서 발급이 정상적으로 수행되었음을 사용자에게 알리게 된다. 따라서 사용자는 인증서의 발급 사실을 인지하게 되어 상기 인증시스템 구비되는 다양한 보안서비스를 상기 인증서를 통해 이용할 수 있게 되는 것이다.

<32> 한편 상술한 본 발명의 설명에서는 구체적인 실시 예에 관해 설명하였으나, 여러 가지 변형이 본 발명의 범위에서 벗어나지 않고 실시할 수 있다. 따라서 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허청구범위에 의해 정하여져야 한다.

【발명의 효과】

<33> 이상에서 설명한 바와 같이, 본 발명은 공개키 기반 인증시스템에서 인증서 발급에 있어서, 인증서 발급 요청시에 요청 메시지의 보호를 위해 발급시 요구되는 인가코드를 등록단계가 아닌 인증서 발급 요청 단계에서 사용자의 생체정보를 통한 사용자 인증시 인증기관으로부터 부여되도록 함으로써 사용자 입장에서

인증서 발급시 복잡한 인가코드를 기억하고 입력하지 않아도 되도록 함으로써 인증서 발급 절차를 간소화할 수 있는 이점이 있으며,

<34> 또한 인증서 발급단계에서 생체정보를 이용하여 인가코드를 부여함에 따라 제3자에 의해 인증서 발급단계 이전에 참조번호가 노출되었다 하더라도 인가코드를 받기 위해서는 생체정보에 의한 실시간 신원확인 절차가 필요하게 되어 제3자에 의한 인증서 발급시도가 방지되어 인증서 발급시 더 높은 보안성을 유지할 수 있게 되는 이점이 있다.

【특허청구범위】

【청구항 1】

등록기관, 인증기관, 사용자 시스템을 포함하는 공개키 기반 구조 인증시스템에서 사용자 시스템과 인증기관간 생체정보를 이용하여 인증서를 발급하는 방법에 있어서,

(a) 인터넷을 통해 상기 인증시스템에 접속한 상기 사용자 시스템으로부터 인증서 발급 요청 메시지를 수신하는 단계;

(b)상기 인증서 발급 요청을 위한 사용자 인증을 위해 상기 사용자 시스템으로부터 전송되는 해당 사용자의 참조번호와 생체정보를 추출하는 단계;

(c) 상기 전송된 사용자의 생체정보와 데이터 베이스 저장부내 등록 저장된 상기 참조번호에 해당하는 회원 등록 사용자의 생체정보가 일치하는지 여부를 검사하는 단계;

(d)상기 생체정보가 일치하는 경우 상기 인증서 요청 사용자의 인가코드를 생성하여 사용자 시스템으로 제공하는 단계;

(e)사용자 시스템으로부터 생성된 공개키를 수신하여 인증서를 발급하는단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급방법.

【청구항 2】

제1항에 있어서,

상기 (d)단계에서, (d1)상기 인가코드를 수신한 사용자 시스템에서 상기 인증시스템에서의 사용을 위한 개인키와 공개키를 생성하는 단계;

(d2)상기 공개키를 인증서 발급을 위해 상기 인증기관 서버로 전송하는 단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급방법.

【청구항 3】

제1항에 있어서,

상기 (e)단계에서 상기 공개키를 수신하는 경우, (e1)상기 공개키를 이용하여 상기 공개키와 키쌍으로 생성되는 사용자의 개인키가 정상적으로 생성되었는지를 검사하는 단계;

(e2)상기 개인키가 정상적으로 생성된 것으로 판단되는 경우 상기 인증서를 발급하는 단계;를 포함하여 진행하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법.

【청구항 4】

제1항에 있어서,

상기 데이터 베이스 저장부는, 상기 인증시스템에 회원 등록된 사용자 정보 및 인증서 발급을 위한 참조번호를 구비한 사용자 정보 DB와 상기 사용자에 대한 생체정보를 저장하고 있는 생체정보 DB를 포함하며, 상기 인증시스템에 등록된 사용자 정보와 해당 사용자의 생체정보를 연계하여 등록 저장하고 있는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 인증서 발급 방법.

【청구항 5】

제1항에 있어서,

상기 사용자 시스템은, 사용자의 생체정보 입력을 위한 생체정보 입력장치를 구비하는 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법.

【청구항 6】

제1항에 있어서,

상기 생체정보는, 상기 사용자 고유의 지문 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법.

【청구항 7】

제1항에 있어서,

상기 생체정보는, 상기 사용자 고유의 홍체 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법.

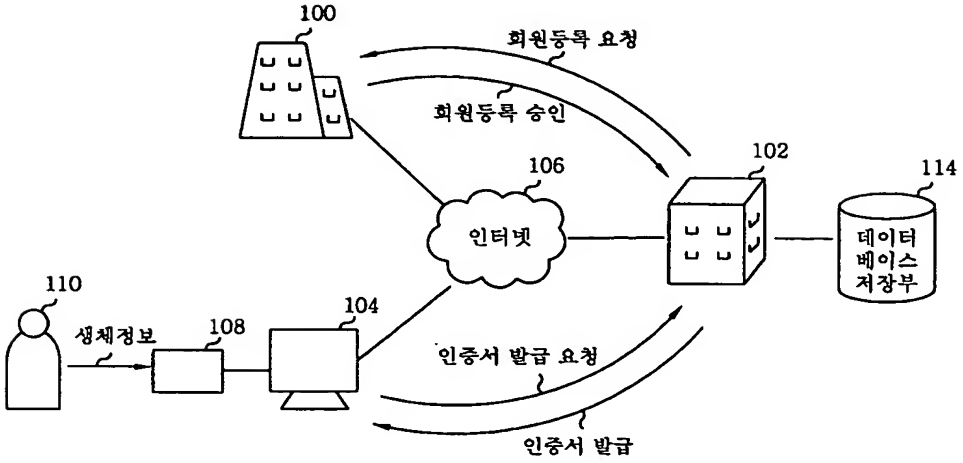
【청구항 8】

제1항에 있어서,

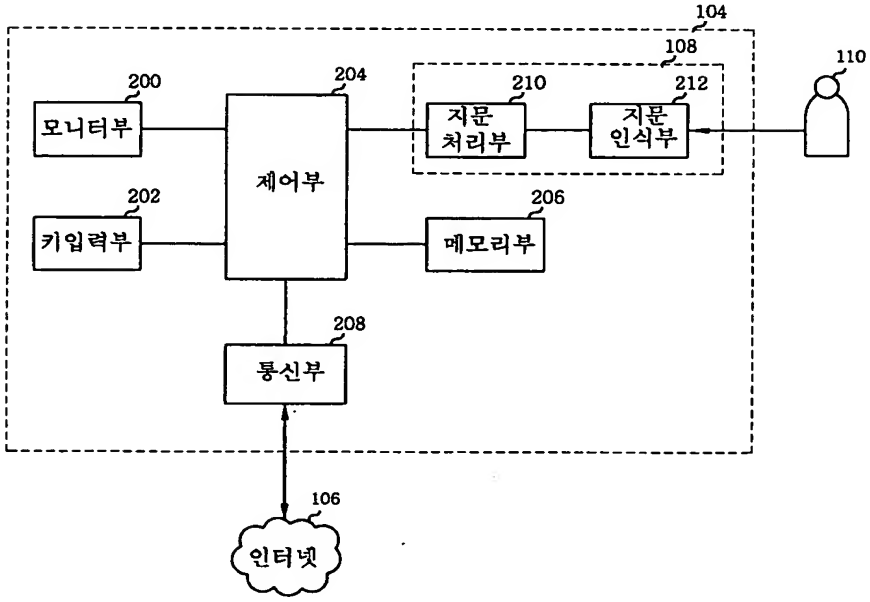
상기 생체정보는, 상기 사용자 고유의 얼굴 특징 벡터 정보인 것을 특징으로 하는 공개키 기반 구조 인증시스템에서 생체정보를 이용한 인증서 발급 방법.

【도면】

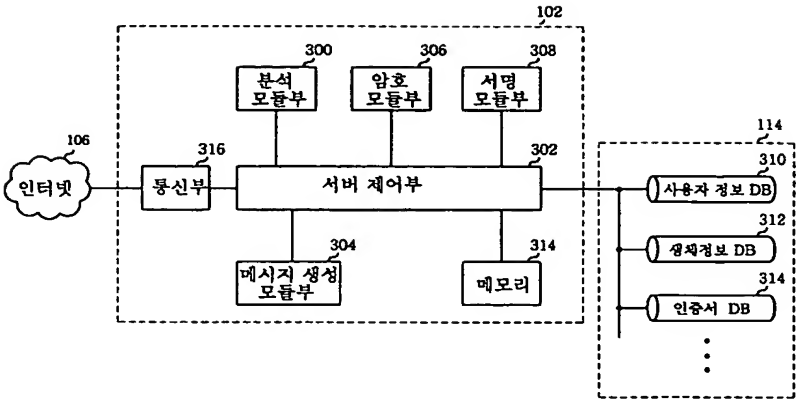
【도 1】


100
회원등록 요청
회원등록 승인
106
인터넷
102
114
데이터 베이스 저장부
110
생체정보
108
104
인증서 발급 요청
인증서 발급

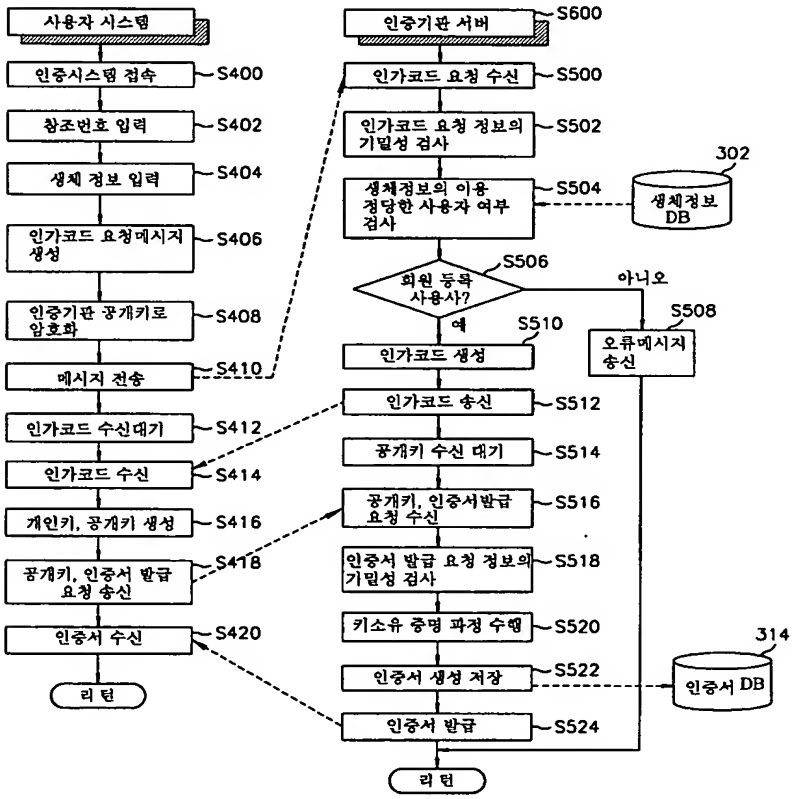
【도 2】


104
108
110
200
모니터부
204
210
지문 처리부
212
지문 인식부
202
키입력부
제어부
206
메모리부
208
통신부
106
인터넷

【도 3】


102
300
분석 모듈부
306
암호 모듈부
308
서명 모듈부
106
인터넷
316
통신부
서버 제어부
302
114
310
사용자 정보 DB
312
생체정보 DB
314
인증서 DB
304
메시지 생성 모듈부
314
메모리

【도 4】


사용자 시스템
인증기관 서버
S600
인증시스템 접속
S400
인가코드 요청 수신
S500
참조번호 입력
S402
인가코드 요청 정보의 기밀성 검사
S502
생체 정보 입력
S404
생체정보의 이용 정당한 사용자 여부 검사
S504
302
생체정보 DB
인가코드 요청메시지 생성
S406
회원 등록 사용자?
S506
아니오
S508
예
S510
인증기관 공개키로 암호화
S408
인가코드 생성
오류메시지 송신
메시지 전송
S410
인가코드 송신
S512
인가코드 수신대기
S412
공개키 수신 대기
S514
인가코드 수신
S414
공개키, 인증서발급 요청 수신
S516
개인키, 공개키 생성
S416
인증서 발급 요청 정보의 기밀성 검사
S518
공개키, 인증서 발급 요청 송신
S418
키소유 증명 과정 수행
S520
인증서 수신
S420
314
인증서 생성 저장
S522
인증서 DB
리턴
인증서 발급
S524
리턴